2009-03

Team 7: Topological Analysis of Infrastructure Network

Soon, SIM Mong

Team 7: Topological Analysis of Infrastructure Network

TEAM 7 MEMBERS

SIM Mong Soon, Ph.D. – Lead
Chin Shi Katt
Lai Kah Wah
Xu Yong Liang
DSO National Laboratories, Singapore

Palvannan Kannapiran
DSTA, SIngapore

Alberto Garcia, LCDR
Naval Postgraduate School, US

Lim Chio Tee
SAF Ops Research Office, Singapore

INTRODUCTION

Critical Infrastructures work together to produce goods and services. For example, the power station generates electricity and the water purification station uses the electricity to produce drinking water. Disruption of Civil Infrastructures will affect our national security, economic well being and way of life. This provides a primary motivation to model and understand the interaction between infrastructures. Based on our works in military modeling and simulation (M&S), we have extended these M&S methodologies to the area of Critical Infrastructure Protection. However, we observed that it take a reasonable amount of modeling effort to model a large network of infrastructures.

There is a need to provide quick answer to operational users. It is sometimes sufficient to have a ballpark estimate of the consequence of a possible disruption in the infrastructure network. This will also assist them to decide on a smaller subset of infrastructures to do detailed modeling and analysis later.

In this workshop, we are proposing to model each infrastructure & its interactions by Network Topology. We implemented this methodology in the NetLogo software. The following sections will discuss our objective for this workshop, describe the scenarios ran during the workshop and highlight some lessons learnt.

DURING THE WORKSHOP

Workshop Objective

In this workshop, we used a case study to evaluate the feasibility of this methodology to model the interaction between infrastructures. The case study here is a military supply chain network model. The initial military supply chain model is developed by Vidal [1]. For the purpose of this workshop, we added some modifications to this model.

The objective is to design a military supply chain with better survivability. The model consists of three types of battalions namely, Main Supply Battalion (MSB), Forward Supply Battalion (FSB) and combat battalion. A MSB supplies goods to a group of FSBs and each FSB in turn feeds the goods to a number of combat battalions. We are interested to determine how different configurations of MSBs, FSBs and battalion will affect the network survivability.

Network survivability

Survivability is defined as Robustness, Responsiveness and Flexibility. Robustness looks at how the size of the network changes when some nodes are removed. Responsiveness measures how quickly some commodities can flow through a network when some nodes are attacked and fail. Flexibility focuses on whether alternate paths exist in a network so that commodity can continue to flow to others nodes after some node failures. To measure these parameters, we have to compute the characteristic path length and the largest component of the network. The characteristics path length calculates the average number of links required to connect each node to every other nodes in the network while the largest component of the network determines the maximum number of nodes that continue to link to each other after some nodes are removed.

To look at how network structures will affect the network survivability, we considered three structures, namely Random network, Scale-free network and UltraLog network. Researchers have already studied the behavior of Random and Scale-free networks under different attack modes. In general, there are two attack modes, random attack and targeted attack. For random attack, the attacker chooses a node to disrupt at random. For targeted attack, the attacker has some information on how the nodes are linked to each other and will choose the most critical node for attack.

In a Scale-free network, when a new node joins the network, the probability that it will attach to an existing node is proportional to the number of links that the node has. Hence, a node with the most number of links is more likely to attract new node. Studies have shown that most real networks behave like the Scale-free network.

A Scale-free network is known to be resilient to random attack but is very vulnerable to targeted attack. This is because in a Scale-free network, there exist a small number of critical nodes with many links. Hence, when the attackers pick a node at random, it is less likely that these critical nodes will be chosen. This intuitively explains the resilient response of the Scale-free network under random attack. However, these critical nodes have a great influence on the survivability of the entire network and when the attackers focus on the critical nodes, the Scale-free network will suffer a serious consequence.

In Random network, nodes are attached to each other randomly. Hence, the response of a random network under

random attack is not much different from that of a targeted attack.

Thadakamalla et al [2] proposed a network topology (herein known as UltraLog network) which is considered a hybrid between a Random network and a Scale-free network. It is suggested that the UltraLog model will be as efficient as the Scale-free network and yet perform better than the Scale-free network under targeted attack.

The UltraLog model is inherently hierarchical in nature. It consists of three layers, namely MSB, FSB and battalion. MSBs, FSBs and battalion enter the system in a certain ratio l:m:n where l > m > n:

a. A MSB has five edges pointing from it.
b. A FSB has three edges pointing from it.
c. A battalion has one edge pointing from it and a second edge added with a probability p.

%MSB	%FSB	%Battalion
3.3	13.3	83.3
6.3	31.3	63.5
7.1	28.6	64.3
8.3	25.0	66.7
10.0	20.0	70.0
9.1	45.5	45.5
11.1	44.4	44.4
14.3	42.9	42.9
20.0	40.0	40.0
12.5	12.5	75.0
20.0	20.0	60.0
33.3	33.3	33.3

Table 1: The configuration simulated during the workshop

Description of Scenario

In this workshop, we relaxed the ratio of MSBs, FSBs and battalion so that l ≥ m ≥ n. Table 1 shows the configurations studied during the workshop.

In addition to network configuration, we also modified the model so that there are four types of attack mode, namely random, targeted attack on critical node, targeted attack on critical node in largest component, targeted attack on critical node in smallest component. For more information on these attack modes, the readers can send the inquiry to the team.

We ran 30 replications of simulation for each configuration type and attack mode. After that, we compared the result with that of Scale-free and Random networks. The number of node used in each replication is 100 and one node is removed from the network at each time step. The simulation stops when 80% of the nodes are removed.

RESULTS AND ANALYSIS

For each configuration and attack mode, we computed the average value of the characteristic path length and the largest component at each time step and plotted them on a graph. Figure 1 and 2 show how the characteristic path length and the largest component behave for the three network structures for a given configuration, under targeted attack on critical node.

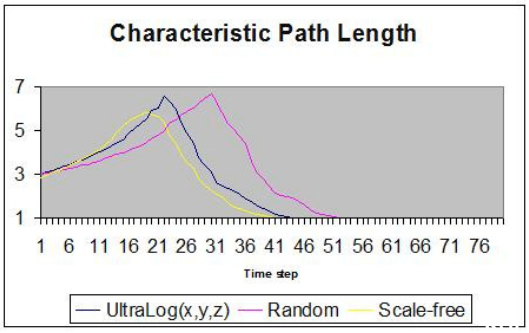

Figure 1: The average characteristic path length at each time step under targeted attack on critical node

In figure 1, it is observed that the rate of increase of the characteristic path length of the Scale-free network is higher than that of the other network structures. Furthermore, the Scale-free network starts to disintegrate at earlier time unit (i.e. time step = 21). On the other hand, the UltraLog model performs better than the Scale-free network but lag behind the random network.

In figure 2, it is again observed that the Scale-free network performs the worst among the three networks. For the Scale-free network, the value of largest component drops at a faster rate than that of the other two networks.

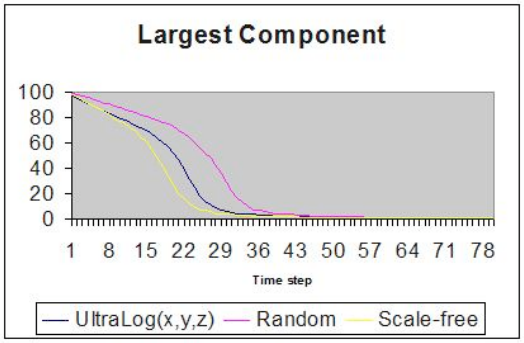

Figure 2: The average largest component at each time step under targeted attack on critical node

For each configuration and attack mode, we plotted the characteristic path length and the largest component for the three networks and made visual comparison. We developed a simple scoring system to assess the performance of the UltraLog network. The following criteria are used to award score to the UltraLog network:

a. Under random attack, if the UltraLog network performs better than the Random network and the Scale-free network, a score of 1 is given.
b. Under random attack, if the UltraLog network performs better than the Random network but lags behind the Scale-free network, a score of 1 is still given.
c. Under targeted attack, if the UltraLog network performs better than the Scale-free network and the Random network, a score of 1 is given.
d. Under targeted attack, if the UltraLog network performs better than the Scale-free network but lags

behind the Random network, a score of 1 is still given.

The result is shown in table 2.

SUMMARY OF FINDINGS

Based on the simulations ran, we observed that the UltraLog model performs better under the following conditions:

1. It is good to have an equal number of MSB, FSB and Battalion but impractical due to high implementation cost.
2. A more practical approach is to have an equal number of FSB and Battalion.
3. We will not recommend an equal number of MSB and FSB

From these observations, a possible rule of thumb is as follows:

Nos. of FSB = Nos. of Battalion > Nos. of MSB

We must caution that these results are obtained from simulations ran during the workshop. It is necessary to check that these observations are true for other configurations that are not ran during the workshop. Furthermore, it will be good to perform the simulation for other network size.

CONCLUSIONS

As conclusion, we found that this approach provide a "good enough" answer for a quick study and highlight some important trends in the result. The data-farming capability of NetLogo software allows the users to run multiple scenarios within reasonable time.

We also made the following improvements to the model:

a. Node recovery. In a real network, a node will recover after a disruption. Hence, it will be more realistic to consider how a node will recover in the model. For the workshop, we have implemented a simple node recovery mechanism.

b. Node replenishment. When a supplier is disrupted, a customer will source for a new supplier. We have also implemented a simple replenishment policy that a node will look for new node to link to, after its supplying node fails.

c. Output analysis. Apart from the capability to run multiple scenarios, the next important step is to facilitate the analysis of this huge amount of simulation outputs. We implemented the analysis tool in VBA and Java.

REFERENCES

[1] The initial military supply chain Netlogo model is developed by Vidal J. M. and is downloadable from: http://jmvidal.cse.sc.edu/netlogomas/

[2] Thadakamalla et al. Survivability of Multiagent-Based Supply Networks: A Topological Perspective. IEEE Intelligent Systems, Sept / Oct 2004.